# MRMCD 2019

Manuel (HonkHase) Atug

# Wie Hackback mit der Gesellschaft spielt

Manuel (HonkHase) Atug

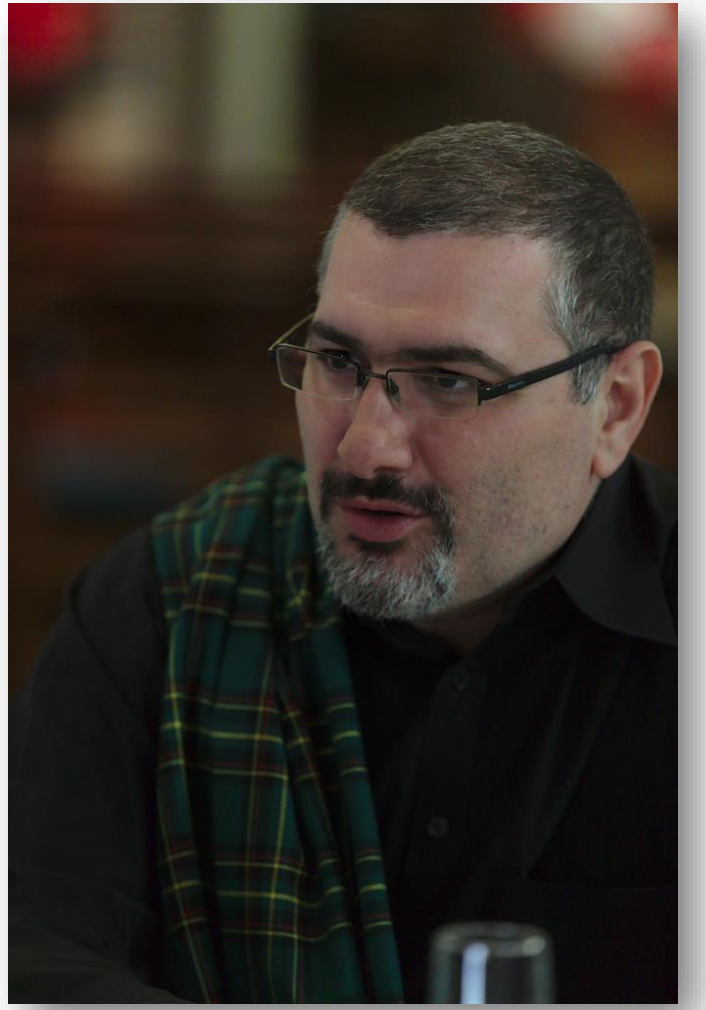
# Manuel (HonkHase) Atug

- Senior Manager bei der HiSolutions AG
- Diplom-Informatiker & Master of Science in Applied IT Security
- seit über 23 Jahren in der Informationssicherheit tätig
- Spezialthemen: KRITIS und Ethik

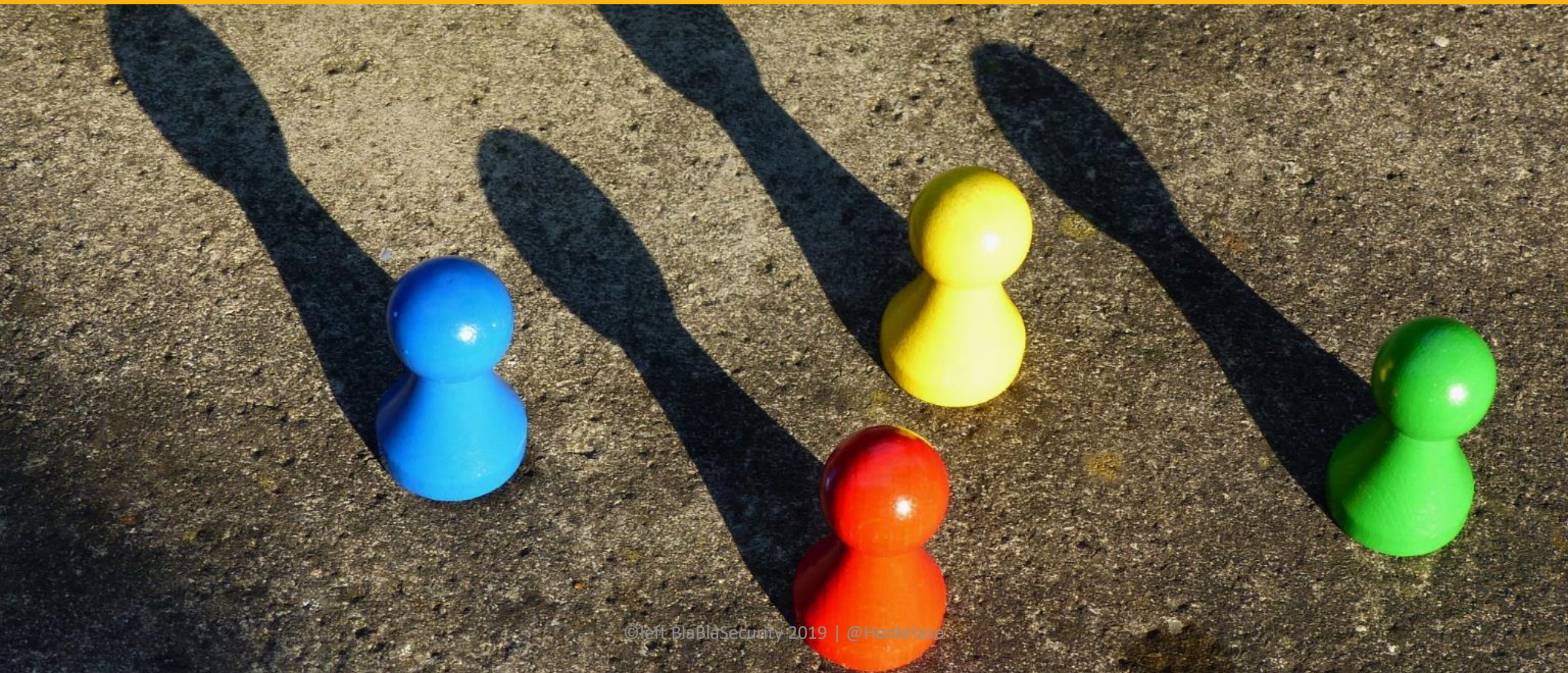
**Seit ~23 Jahren Aktiv in so n paar Vereinen:**

- Chaos Computer Club e.V., Chaos Computer Club Cologne e.V., c-base e.V., Digitale Kultur e.V., ISACA, GI e.V., FIfF e.V., Freie Software Freunde e.V., Geraffel Core Member
- Leitung der AG KRITIS: https://ag.kritis.info
- @HonkHase

AG KRITIS



# Hackback-Quartett

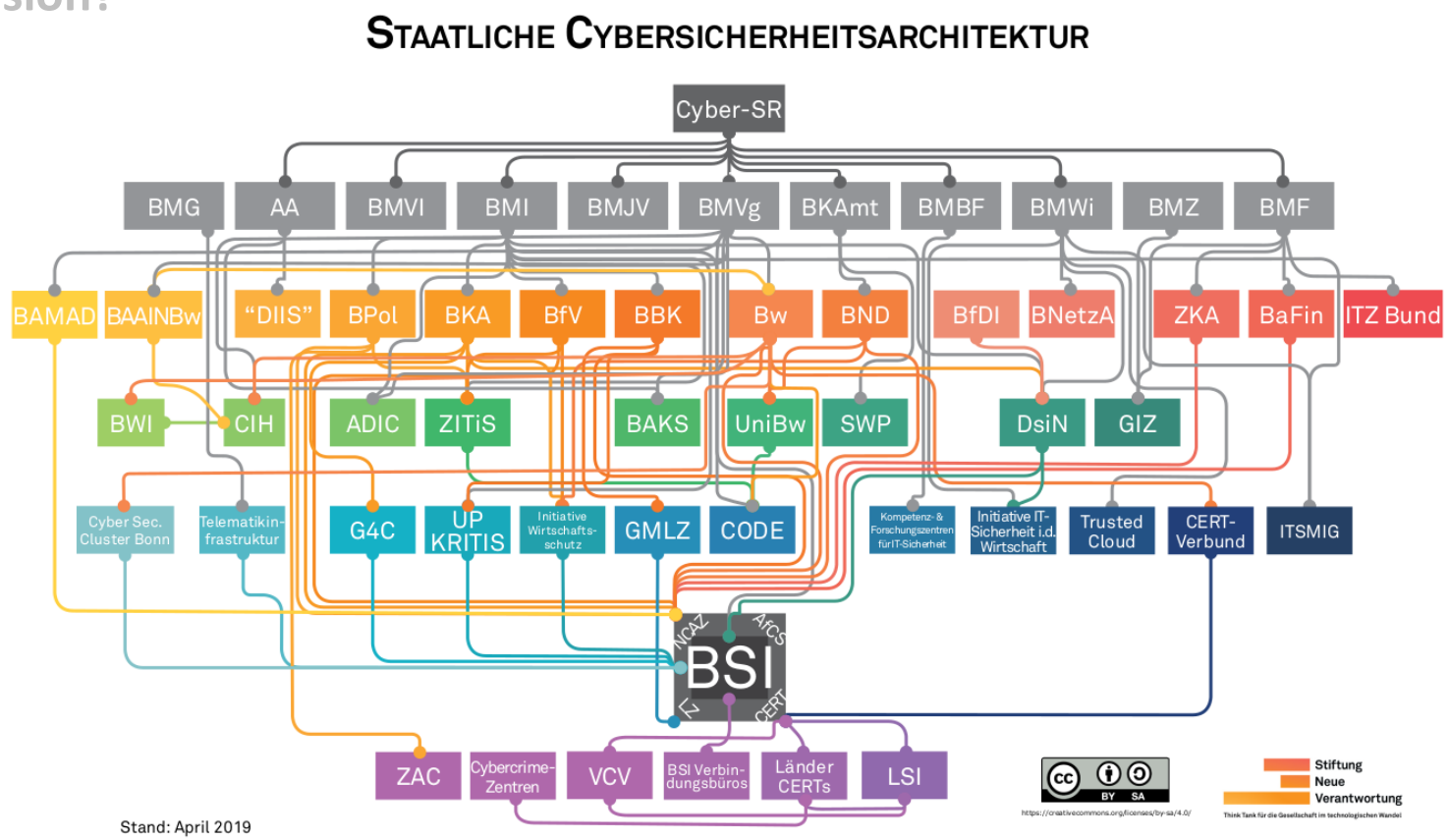


# Was ist ein Hackback?

- Fragestellung der deutschen (Sicherheits-)Behörden:
  - Wie reagiert man offensiv auf Cyber-Angriffe?
- aka known as
  - “Digitaler Gegenangriff”
  - “Aktive Cyberabwehr”
  - “finaler digitaler Rettungsschuss”
  - …
- Die aktuelle Regierung erarbeitet einen Gesetzgebungsvorschlag aus… seit Jahren

# Bei wem Cybert‘s hier eigentlich?

Verantwortungsdiffusion?




Quelle: Stiftung Neue Verantwortung

Organisationssoziologie!

# Gesetzgebung zu Hackback

- Alles halt nicht so einfach…
  - Völkerrecht
  - Grundrecht
  - Genfer Konventionen

- Legal… Illegal… Ikearegal…

# Rechtlicher und organisatorischer Rahmen?

- Rechtliche Fragen zu Hackback und aktive Cyberabwehr sind seit Jahren in Arbeit
- Bundesregierung (Drucksache 19/11920) geht von **digitalen Waffen** auf Kritischen Infrastrukturen (KRITIS) in Deutschland aus

➔ Kauf & Entwicklung von digitalen Cyberwaffen durch die Bundesregierung wird explizit nicht verneint. „nur deren Einsatz“

# Digitale Waffen?!

- Unterschied **Security Research** und **D-Waffen**?
  - nicht die technische Schwachstelle, sondern das Ziel!

- Forschung endet z.B. bei der Remote Code Execution (durch ausführen von calc.exe)
- Forschung biegt dann ab, Richtung Mitigation

- **D-Waffen** Entwicklung fängt dann erst richtig an…

# Wer macht denn dann so einen Hackback?

- Bundesnachrichtendienst (BND)?
  - Nachrichtendienst für die Auslandsaufklärung
- Verfassungsschutz (BfV)?
  - Nachrichtendienst für die Inlandsaufklärung


Verfassungsrechtliches Trennungsgebot

➔ Aufgrund Erfahrungen mit Gestapo im Dritten Reich

➔Deutsche Nachrichtendienste dürfen daher nur Informationen sammeln und auswerten, keine Cyberangriffe durchführen

# Wer macht denn dann so einen Hackback?

- Bundeskriminalamt (BKA)?
  - Nationale Kriminalitätsbekämpfung


- Bundespolizei (BPOL)?
  - Sonderpolizeiliche Aufgaben


➔Ermitteln nur bei Computerstraftaten

➔Unter Einsatz von Quellen-TKÜ und Staatstrojanern

# Wer bleibt übrig für so einen Hackback?

- Streitkräfte der Bundesrepublik Deutschland (Bundeswehr + MAD und so)!?!
- Naja, wenn die Bundeswehr tätig werden soll, muss es sich um einen Spannungsfall oder Verteidigungsfall handeln. Immer. Also wirklich immer. Echt jetzt immer.

BUNDESWEHR

➔ Art. 87a (2) GG:
*Außer zur Verteidigung dürfen die Streitkräfte nur eingesetzt werden, soweit dieses Grundgesetz es ausdrücklich zuläßt.*


- Verteidigungsfall ➔ Reaktion auf eine militärische Gewaltanwendung, die von außen kommt

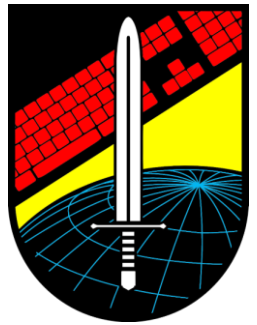
# Cyberwar und Hackback können wir!

# Hyper^^Cyber! Cyber!

- KDOCiR (Kommando Cyber- und Informationsraum)
  - Zentrum Cyber Operationen (ZCO)
    - Kernauftrag des ZCO ist das Planen, Vorbereiten und **Führen** von Cyber-Operationen (CO) zur Aufklärung und **Wirkung** (durch Cyber-Wirkketten)

Interne Verbands-abzeichen:

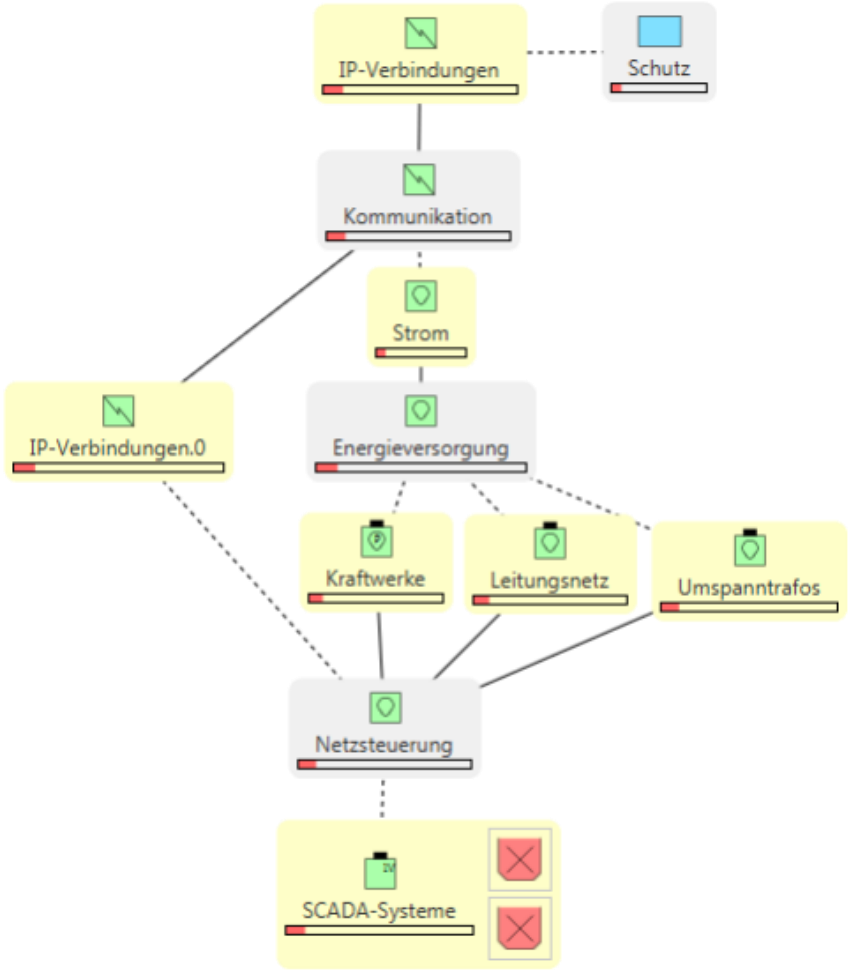
KDOCiR



ZCO

# Cyber-Wirkketten?

- **Cyberwirkung** löst häufig eine Kettenreaktion auf dem **Fähigkeits-Ressourcen-Netzwerk** aus
  - Angriff auf **SCADA-System** führt zum Ausfall der **Stromversorgung**
  - Ausfall der **Stromversorgung** führt zum Ausfall der **Telekommunikation**
  - Ausfall der **Telekommunikation** führt zum Ausfall/Einschränkung von **Schutzfunktion**



# Cyber-Wirkmittel?

## Annahme

# Cyber-Wirkmittel!

KdoCIR

## Cyber-Wirkmittel

Globale Reichweite bei sofortiger Wirkung ohne Vorwarnzeit

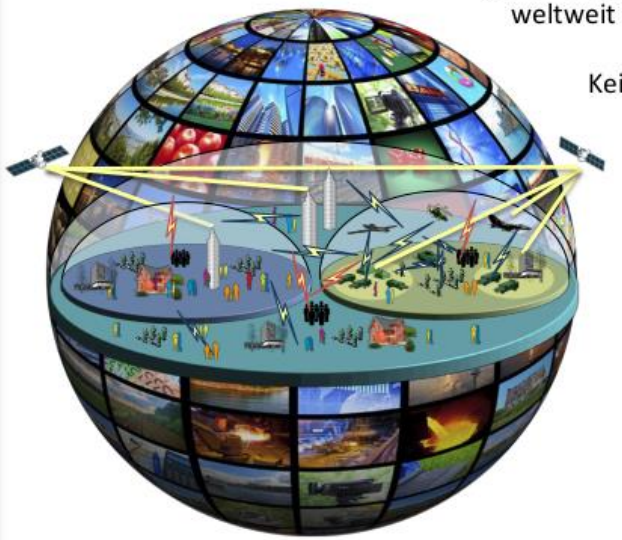
Hohe Wirkbreite ähnlich zu ABC-Wirkmitteln

Hohe Genauigkeit bei gleichzeitiger Bekämpfung weltweit verteilter Ziele

Reversible Wirkung bei minimalem Kollateralschaden

Kein Exponieren des Angreifers beim Einsatz der Wirkmittel

Langer Vorlauf durch notwendige Eindring-/ Ausbring-Phase



ähnlich einer Neutronenwaffe ohne Fall-Out

CIR CYBER- UND INFORMATIONSRAUM OFFEN Folie 12

Na sag ich doch… das KDOCiR auch!

# Cyber-Optionen im militärischen Umfeld

- Cyber-Optionen
  - **Spionage**
  - **Beeinträchtigung** der Führungsfähigkeit
  - **Sabotage** Kritischer Infrastrukturen (KRITIS)
  - **Defacement** von regierungseigenen Webseiten und offiziellen Kommunikationswegen
  - **Desinformation** über soziale Medien
  - **Blockade** des nationalen Zugangs zum Internet

# Charakteristik Hybrider Bedrohungen

- **Unterhalb der Schwelle eines bewaffneten Konflikts**
- **Verschleierung** der Urheberschaft zur Vermeidung der Attribution
- Konzertierte **Desinformationspolitik**
- **Destabilisierung** einer Gesellschaft von innen

# Cyberwar und Hackback

- Gelebt wird eine **wissenschaftsfeindliche Sicherheitspolitik** (wie bei der Klimapolitik)
- Resultat: Mehr Security?
- Nope -> mehr Cyber**UN**sicherheit

# Ach komm… wissenschaftsfeindliche Sicherheitspolitik?

## *Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung*


- Der **Wissenschaftliche Dienst** sagt „Die Bundesregierung arbeitet an offensiven Kapazitäten und Hackbacks, doch das ist **ineffektiv** und **gefährlich**.“
- Entwickelt hat es Dr. John Zimmermann **Oberstleutnant** der Bundeswehr
- Steht seit **über 30 Jahren** im Dienst der Bundeswehr
- Es wurden **wesentliche Teile** der Forderungen der **AG KRITIS** bestätigt

Das **Gutachten** wurde auf **netzpolitik.org** veröffentlicht.

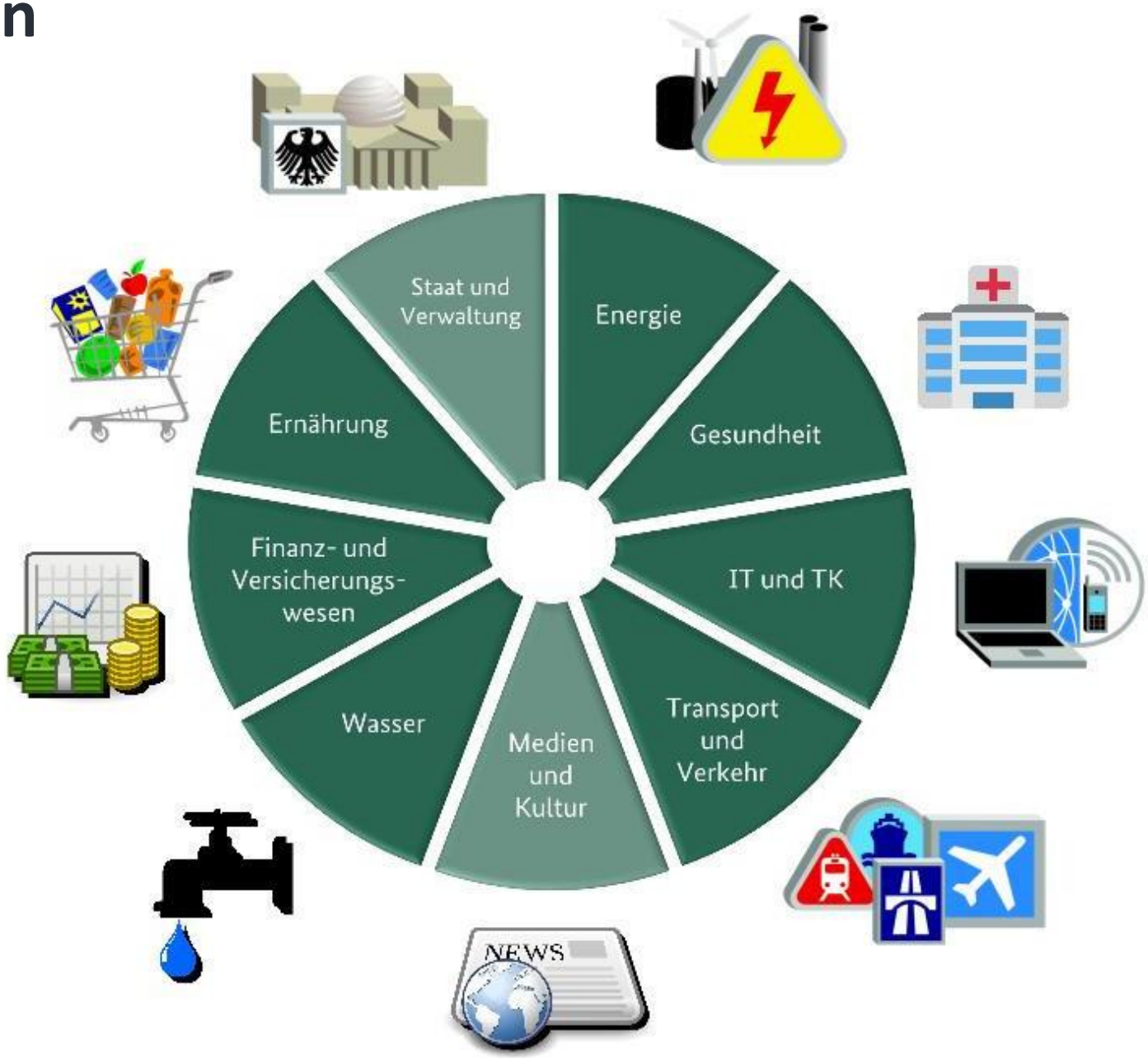
18 Seiten harter Tobak!

NETZPOLITIK.ORG

Quelle: https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/#spendenleiste

# Wieso #Defensive statt #Offensive am Beispiel von KRITIS

# KRITIS Sektoren




Quelle: BSI


- KRITIS: primär Schutz der Bevölkerung, nicht des Betreibers
- Kritische Infrastrukturen: oftmals identische Komponenten
- Vernetzung: Immer mehr Komponenten werden an das Internet verbunden
- Durch den Staat zurückgehaltene 0day Lücken in kritischen Infrastrukturen bedrohen die Bevölkerung
- Cyberabwehr in Defensive statt „aktive Cyberabwehr“ in Offensive (Hackback), so dass kritische Infrastrukturen nicht gefährdet, sondern geschützt werden

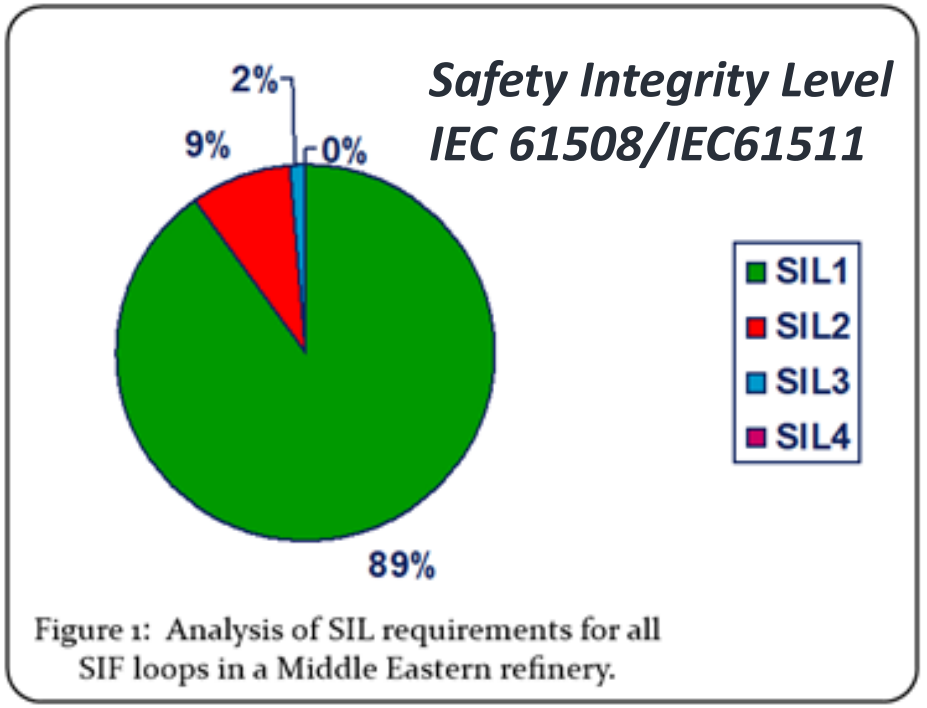



Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.


Triconex Tricon

Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

## Attacken auf das Ukrainische Stromnetz

- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld

## Attacke auf Saudi Arabisches Kraftwerk

- TRITON: passiver Implant mit Remote Access Funktion
- Folge wäre gewesen: Explosionen und die Freisetzung von Schwefelwasserstoffgas

# Und nun?

- Unabhängigkeit des BSI vom BMI
- Strikt defensive Cybersicherheitsstrategie
- Ächtung von ABCD-Waffen (inkl. Digitalen Waffen)
- Evaluierung der vorhandenen Gesetze und Maßnahmen
- Bevölkerungsschutz durch Behebung von Schwachstellen durch Hersteller

# Defensive Cybersicherheitsstrategie

- Bei KRITIS eingesetzte Software grundsätzlich als Open Source oder Quellcode in treuhänderischer Verwaltung
- Bildungspolitik: Sichere(!) Quellcode-Entwicklung ausbilden
- Keine Bereitstellung von Budgets für staatliche Akteure, um 0days zu kaufen oder zu entwickeln
- Verpflichtung für staatliche Akteure, ihnen bekannt gewordene Schwachstellen über ein unabhängiges BSI an den Hersteller zu melden

# Unabhängigkeit des BSI

Evaluierung möglicher Optionen:
(fachliche Unabhängigkeit, starke Unabhängigkeit, andere Abhängigkeit, Digitalministerium, …)

Vielversprechende Option: § 1 BSIG Änderung zur Grundlage technisch-wissenschaftlicher Erkenntnisse

*„Das BSI führt seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen der jeweils fachlich zuständigen Ministerien durch.“*

# What‘s Next?

@HonkHase

HonkHase@kritis.info

www.blablasecurity.de

ag.kritis.info

AG KRITIS